(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 March 2004 (11.03.2004)

PCT

(10) International Publication Number
WO 2004/021638 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2003/026834

(22) International Filing Date: 28 August 2003 (28.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/406,721 28 August 2002 (28.08.2002) US
60/412,221 20 September 2002 (20.09.2002) US

(71) Applicant *(for all designated States except US)*: DOCOMO COMMUNICATIONS LABORATORIES USA, INC. [US/US]; 181 Metro Drive, Suite 300, San Jose, CA 95110 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: GENTRY, Craig [US/US]; 230 Houghton St., Mountain View, CA 94041 (US).

(74) Agent: HORIE, Tadashi; Brinks Hofer Gilson & Lione, P.O. Box 10087, Chicago, IL 60610 (US).

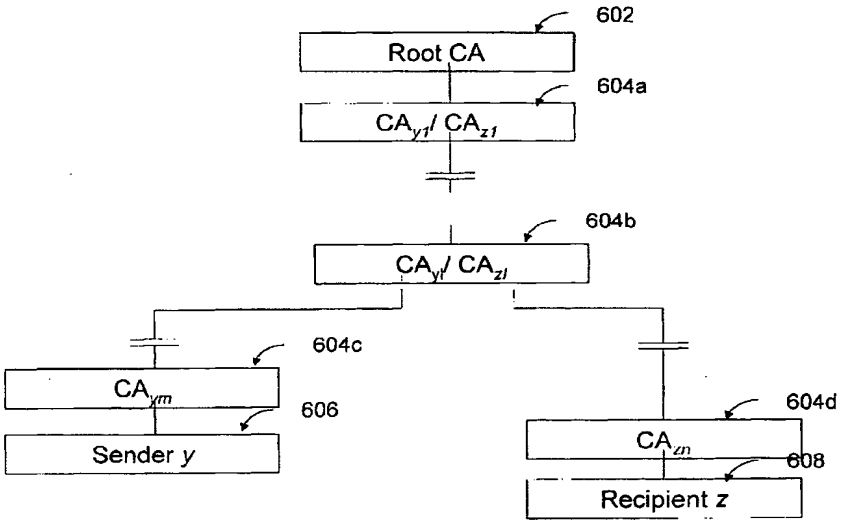
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: CERTIFICATE-BASED ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE



(57) Abstract: The present invention provides methods for sending a digital message from a sender (606) to a recipient (608) in a public-key based cryptosystem comprising an authorizer (606). The authorizer can be a single entity (606) or comprise a hierarchical or distributed entity (602, 604a-604b). The present invention allows communication of messages by an efficient protocol, not involving key status queries or key escrow, where a message recipient (608) can decrypt a message from a message sender (606) only if the recipient (608) possesses up-to-date authority from the authorizer. The invention allows such communication in a system comprising a large number (e.g. millions) of users.

WO 2004/021638 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/26834

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/156, 157
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/156, 157

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,867,578 A (BRICKELL et al) 02 February 1999 (02.02.1999), abstract; fig.1 and 3; col.3, lines 44-67; col.4-29.	1-8, 16, 18-25, 27, 28 and 68-71
Y	US 5,774,552 A (GRIMMER) 30 June 1998 (30.06.1998), abstract; fig.1-5 and 13; col.2, lines 43-67; col.3-7 and col.8, lines 1-33.	1-8, 16, 18-25, 27, 28 and 68-71

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 2004 (16.01.2004)	03 FEB 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron Telephone No. 703-305-3900